ソフトウェア製品セキュリティ情報
Software Vulnerability Information

ソフトウェア事業部 (Software Division)

2003.07.07更新

SQL Server 2000 および Microsoft Desktop Engine 2000 (MSDE 2000) に関するセキュリティ問題の説明

- 影響がある製品

対策	製品名	適用ＯＳ	更新日
HS02-013-01	JP1/VERITAS Backup Exec 9.0 for Windows Servers	Windows	2003.02.12
HS02-013-02	RealSecure WorkGroup Manager，System Scanner，RealSecure SiteProtector，RealSecure ICEcap Manager	Windows	2003.02.07
HS02-013-03	JP1/VantagePoint Internet Services	Windows	2003.02.21

- 問題の説明

2002.07.29，米国CERT/CCからMicrosoft SQL Server 2000 および Microsoft Desktop Engine 2000 (MSDE 2000) に関するセキュリティ問題（Advisory CA-2002-22) が公表されました。

（Microsoft からは2002.07.25，セキュリティ情報： MS02-039 で公開）

これは，SQL Server 2000，および SQL Server 2000 の派生製品

＞ トップ
What's New
＞ お知らせ
＞ 御参考（警告情報など）
＞ ソフトウェア製品セキュリティ情報
＞ セキュリティ対応機関へのリンク

＞ お問い合わせ
soft-security @itg.hitachi.co.jp

にあたるMSDE 2000という組込み型のソフトウェア部品において，バッファオーバーランおよびサービス拒否の脆弱性が確認されたもので，SQL Server 2000 以外でも MSDE 2000 を組み込んだソフトウェア製品も，本脆弱性に該当します。
これらの脆弱性により，SQL Serverサービスが異常終了したりセキュリティ コンテキストで任意のコードを実行される恐れや，サービス拒否攻撃を受けることでシステムのパフォーマンスが著しく低下する恐れがあります。

対策パッチ適用が完了するまでは，お客様のシステムにおいて以下の対策を実施いただくことを推奨いたします。

1. UDPポート 1434番への信頼できないホストからの通信トラフィックを遮断するよう，ルータ等のネットワーク機器およびサーバにおいて設定する。

[ご参考 : Slammer/SQL Exp ワームについて]

2003.01.25頃より新聞紙上等で取り上げられている Slammer/SQL Exp ワームについて，SQL Server 2000が稼動しているサーバに感染するということが知られています。このワームは，SQL Server 2000 の派生製品にあたるMSDE 2000についても感染の対象となることが判明しており，MSDE 2000を組み込んだソフトウェア製品も影響を受ける可能性があります。

（CERT Advisory CA-2003-04 MS-SQL Server Worm）

- SQL Server 2000の対策については，MicrosoftのWebサイトを参照ください。SQL Server 2000に対応した弊社ソフトウェア製品の情報は，Windowsセキュリティパッチへのサポート状況を参照ください。

- MSDE 2000を組み込んだ弊社ソフトウェア事業部より提供している製品については，影響を受ける製品および対策版の情報を当ページで提供してまいります。

更新履歴 ：

- 2003.07.07 : このセキュリティ情報ページをリニューアルしました。

- 弊社では，セキュリティ対応に関して正確な情報を提供するよう努力しておりますが，セキュリティ問題に関する情報は変化しており，当ホームページで記載している内容を予告なく変更することがありますので，あらかじめご了承ください。情報ご参照の際には，常に最新の情報をご確認いただくようお願いします。
- 当ホームページに記載されている製品には，他社開発製品が含まれております。これらのセキュリティ情報については他社から提供，または公開された情報を基にしております。弊社では，情報の正確性および完全性について注意を払っておりますが，開発元の状況変化に伴い，当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ

トップ
What's New
お知らせ
御参考（警告情報など）
ソフトウェア製品セキュリティ情報
セキュリティ対応機関へのリンク

お問い合わせ
soft-security
@itg.hitachi.co.jp

2003.07.07更新

HS02-013;

SQL Server 2000 および Microsoft Desktop Engine 2000 (MSDE 2000) に関するセキュリティ問題の説明

JP1/VERITAS Backup Exec 9.0 for Windows Servers の対策

JP1/VERITAS Backup Exec 9.0 for Windows Serversは、内部のデータベースコンポーネントとしてMicrosoft社のMSDE 2000（英語版）を使用しています。2003年1月に発生したコンピュータウィルス “SQL Slammer ワーム” は、当該コンポーネントにも作用することが判明しています。
JP1/VERITAS Backup Exec 9.0 for Windows Servers のインストールもしくはアップグレード後、以下の対策を必ず実施してくださいますようお願いいたします。また、JP1/VERITAS Backup Exec 9.0 for Windows Serversでは、ExecViewは当面サポート対象外とさせていただきます。

1. 影響のある製品

品名：JP1/VERITAS Backup Exec 9.0 for Windows Servers 06-72

形名：RT-1V25-K1W110 /K1WS10 / K1WS40 /K1WL10 /K1WU10 /K1WS20 / K1WU20 /K1WS30

2. 対策

JP1/VERITAS Backup Exec 9.0 for Windows Serversと共にインストールされるMSDE 2000（英語版）コンポーネント に、Microsoft社より提供されるMSDE 2000（英語版）用のパッチを適用してください。詳細は以下URLをご覧ください。

VERITAS Software Corprationの情報発信ページ
URL：http://seer.support.veritas.com/docs/254245.htm
（VERITAS Software Corprationのホームページにリンクします）

3. 対策手順

(1) 上記のVERITAS社の情報発信ページよりリンクされているMicrosoft社の対策パッチ（MS02-039 Patch）をダウンロードします。

MS02-039 Patch: Buffer Overruns in SQL Server 2000 Resolution Service Might Enable Code Execution
Q323875_SQL2000_SP2_en.EXE

(2) 適用対象のシステムにワークディレクトリを作成し、パッチファイルを格納します。

(3) パッチファイルをダブルクリックし、実行します。解凍先ディレクトリを聞かれるため、適切なディレクトリを入力もしくは選択します。解凍を実行すると、四つのファイルが展開されます。

(4) SQLサービスを停止します。プログラムメニューより、[管理ツール] → [サービス]を選択します。サービスウィンドウより、次の二つのサービスが開始されている場合は停止します。

MSSQL$BKUPEXEC SQLAgent$BKUPEXEC

(5) SQL Serverの該当するファイルの退避を行います。

(Program filesフォルダ)¥ Microsoft SQL Server ¥ MSSQL$BKUPEXEC ¥ Binn¥ SSnetlib.dll を適当な名称にリネームします。

(6) 解凍されたファイルから ssnetlib.dll を、 (Program filesフォルダ)¥ Microsoft SQL Server ¥ MSSQL$BKUPEXEC ¥ Binn ¥ へコピーします。

(7) システムを再起動します。

(8) (2)および(3)で作成したファイルを削除します。

更新履歴 ：

- 2003.07.07 : このセキュリティ情報ページをリニューアルしました。

の記載内容に変更が生じることがあります。

- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ

ソフトウェア製品セキュリティ情報
Software Vulnerability Information

ソフトウェア事業部 (Software Division)

2003.07.07更新

HS02-013;

SQL Server 2000 および Microsoft Desktop Engine 2000 (MSDE 2000) に関するセキュリティ問題の説明

RealSecure の対策

RealSecure製品群において、SQL Server 2000 または MSDE 2000(Microsoft Desktop Engine 2000) を利用した環境でのSQL Slammer Wormへの対応について提示させていただきますので留意の上、ご利用いただきますようお願いいたします。

１．影響のあるRealSecureの形名/バージョン

１． １ MSDEを同梱している製品

形名 製品名 バージョン

・R-1V11-RWGMP RealSecure WorkGroup Manager 6.0，6.5

・R-1V11-RWGMSP RealSecure WorkGroup Manager 6.0，6.5

・R-1V11-RSPSP RealSecure WorkGroup Manager Scalability Pack 6.0，6.5

トップ

What's New

お知らせ

御参考（警告情報など）

ソフトウェア製品セキュリティ情報

セキュリティ対応機関へのリンク

お問い合わせ

soft-security @itg.hitachi.co.jp

１． ２ SQL Server 2000、MSDE 2000を前提とする製品

形名 製品名 バージョン

・R-1V11-S2S1P System Scanner 1 device pack 4.0，4.1，4.2

・R-1V11-S2S5P System Scanner 5 device pack 4.0，4.1，4.2

・R-1V11-S2S10P System Scanner 10 device pack 4.0，4.1，4.2

・R-1V11-S2S20P System Scanner 20 device pack 4.0，4.1，4.2

・R-1V11-S2S30P System Scanner 30 device pack 4.0，4.1，4.2

・R-1V11-S2S50P System Scanner 50 device pack 4.0，4.1，4.2

・R-1V11-S2S75P System Scanner 75 device pack 4.0，4.1，4.2

・R-1V11-S2S100P System Scanner 100 device pack 4.0，4.1，4.2

・R-1V11-S2S150P System Scanner 150 device pack 4.0，4.1，4.2

・R-1V11-S2S200P System Scanner 200 device pack 4.0，4.1，4.2

・R-1V11-RSSPP RealSecure SiteProtector 1.2

・R-1V11-BM1P RealSecure ICEcap Manager 1 License 2.6，3.0，3.1

・R-1V11-BM5P RealSecure ICEcap Manager 5 License 2.6，3.0，3.1

・R-1V11-BM10P RealSecure ICEcap Manager 10 License 2.6，3.0，3.1

２．Microsoft SQL Slammer Wormへの対応方法

マイクロソフト社から提供されているSQL Server2000用サービスパック(MSDE用サービスパックを含む)を適用願います。

サービスパックの適用方法については、ISS社のナレッジベースを参照してください。

ISS社のナレッジベースのURL

<http://www.isskk.co.jp/support/index_KB.html>

上記URLにアクセス後、「ナレッジベース」をクリック、さらに「FAQを検索」をクリックします。

以下の条件にて検索してください。

検索テキスト → 030127-000000 を入力

検索条件 → プルダウンメニューから「リファレンス番号」を選択

SQL Server2000用パッチ(MSDE用パッチを含む)の適用方法及び適用手順
については、ISS社のナレッジベースを検索後、
・「2) SQL Server2000及びMSDE2000へのサービスパック適用について」
・添付ファイル「SP適用方法と結果.pdf」
を参照してください。

更新履歴 ：

- 2003.07.07 : このセキュリティ情報ページをリニューアルしました。

行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。

- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ

トップ

What's New

お知らせ

御参考（警告情報など）

ソフトウェア製品セキュリティ情報

セキュリティ対応機関へのリンク

お問い合わせ
soft-security
@itg.hitachi.co.jp

個人情報保護ポリシーにご同意頂ける場合のみ、上記アドレスをご利用下さい。ご同意頂けない場合には、お問い合わせに回答できない場合があります。
なお、入力頂いた個人情報は本ポリシーに従って適切に管理し、問合せ対応のためにのみ使用します。第三者への個人情報の提供、預託、開示は法令に基づく場合を除いて行いません。
お問い合わせへの回答後、個人情報は当社が責任を持って適切に廃棄いたします。

日立および他社の商品名称に関する記述

2003.07.07更新

HS02-013;
SQL Server 2000 および Microsoft Desktop Engine 2000 (MSDE 2000) に関するセキュリティ問題の説明

JP1/VantagePoint Internet Services の対策

1. 影響のあるバージョン

P-242C-5264 JP1/VantagePoint Internet Services 06-71

※ 06-50～06-51(およびそれぞれの修正版を含む)は，MSDE 2000 を含んでいないため，影響ありません。

[注意事項]
以下のいずれかの条件で 06-71 をインストールした場合，MSDE 2000 はインストールしませんので，本対策は不要です。

(1) 06-51-/A からのバージョンアップ(上書きインストール)をした場合。

(2) 06-71 をインストール時，インストールするマシンに SQL Server

7 がインストールされていた場合。

MSDE 2000 がインストールされているか否かは，次の方法で確認できます。

- 「スタート」→「設定」→「コントロールパネル」→「管理ツール」→「サービス」で「サービス」を開き，「MSSQL$OVOPS」サービスが登録されていれば，MSDE 2000 がインストールされています。

2. マイクロソフト社から提供されている MSDE 2000 用パッチについて

マイクロソフト社から提供されております MSDE 2000 用のパッチ(SP3)につきましては，当初，弊社該当製品において適合性が確認されてなく，弊社製品自体のパッチが必要となる可能性もあったため，動作確認を行なっておりました。 その結果，弊社製品側のパッチは不要であり，すべてマイクロソフト社から提供されているパッチ(SP3)の日本語版をそのままご利用いただけることが判明いたしました。

3. 対策パッチ適用手順

下記に従い，MSDE 2000 SP3 を適用願います。（日本語版を適用。英語版は適用不可）
なお，弊社製品自体の対策版の提供はありません。

形名	対象バージョン	適用OS	対策パッチ			更新日
			適用手順		ダウンロード	
P-242C-5264	06-71	Windows	HS02-013-03-a	PDF版(557KB)	MicroSoft社サイト	2003.02.21

4. 注意事項

ここに記述してある対策方法は，2003.02.21現在のものです。なお，今回適用するパッチはすべてマイクロソフト社から提供されております。弊社からの適用手順とともに，マイクロソフト社から提供されている当該パッチ関連情報を必ずお読みの上，作業を行ってください。

更新履歴 :

- 2003.07.07 : このセキュリティ情報ページをリニューアルしました。
- 2003.01.31 : このセキュリティ情報ページを公開しました。
- 2003.02.19 : この問題の対策方法として，MSDE 2000 SP3 が適用可能であることをお知らせしました。
- 2003.02.21 : 手順書の冒頭に，本対策方法は2003.02.21現在のものである旨の注意を記載しました。

行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。

- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ